

在脱机Catalyst 9300X系列交换机上使用SLP配置HSEC许可证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[关闭智能许可传输。](#)

[安装信任ACK请求](#)

[将信任请求文件上传到思科SSM并下载ACK文件。](#)

[CopyTrust ACK文件](#)

[导入该文件并将其安装在产品实例上。](#)

[安装包含所有必需信息的授权请求。](#)

[将授权请求文件上传到思科SSM并下载ACK文件。](#)

[CopyAuthorization RequestACK文件](#)

[安装授权请求ACK文件](#)

[验证](#)

简介

本文档介绍如何在脱机Catalyst 9300X系列交换机上使用SLP配置HSEC许可证。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解使用策略(SLP)的思科智能许可概念
- 熟悉Cisco Catalyst 9300X系列交换机硬件和软件管理
- 在思科智能软件管理器(CSSM)中导航和管理许可证的经验
- 能够在Cisco IOS XE设备上使用CLI
- 了解思科DNA许可证授权类型
- 设备注册和许可证保留的程序

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Hardware:思科Catalyst C9300X-24Y
- 软件：思科IOS XE 17.12.04
- 智能许可基础设施：思科智能软件管理器(CSSM)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

HSEC（高安全性）许可证可在思科平台上实现高级安全功能，增强网络保护、数据完整性和隐私性。它提供强大的工具，用于安全通信并符合严格的安全要求。

HSEC支持的主要功能包括：

- VPN支持可促进公共网络（例如IPsec和SSL VPN）之间安全、加密的通信，以实现站点到站点和远程访问。
- 加密功能支持强大的加密算法进行数据保护，包括用于确保机密性、完整性和身份验证的AES和SHA。
- WAN MACsec可跨广域网链路扩展第2层加密(MACsec)功能，从而确保非受信任网络上的端到端数据安全。
- 可扩展性增强功能可释放加密隧道（例如VPN会话）的更大规模，以支持大型部署。
- 安全通信支持FlexVPN和DMVPN等功能，实现动态、可扩展且安全的连接。

配置

使用C9300X CLI配置智能许可。

关闭智能许可传输。

CLI 配置：

```
device#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
device(config)#license smart transport off
```

安装信任ACK请求

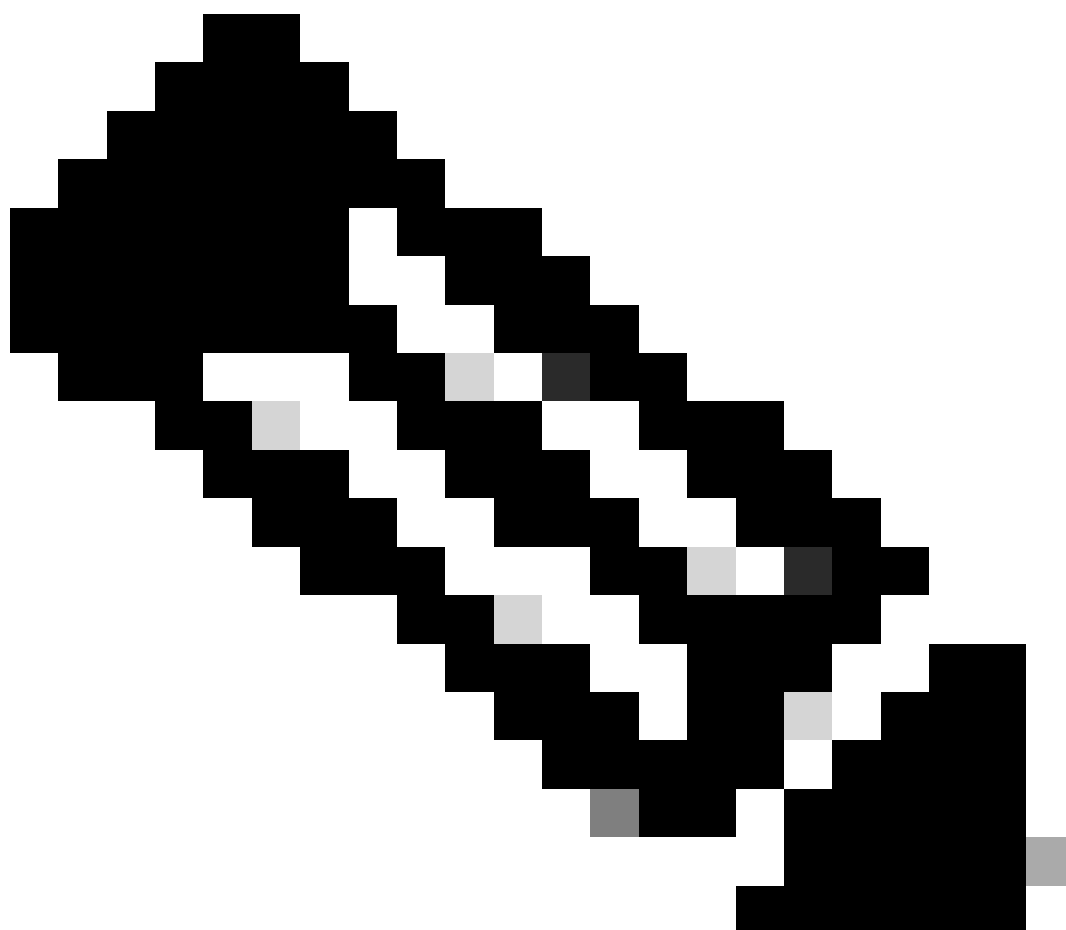
为闪存中的活动产品实例生成并保存信任代码请求。

CLI 配置：

```
device#license smart save trust-request flash:trust_request.txt
```

将信任请求文件上传到思科SSM并下载ACK文件。

1. 登录Cisco SSM Web UI，网址为<https://software.cisco.com>。在智能软件许可下，单击管理许可证链接。
 2. 选择接收报告的智能帐户。
 3. 选择Smart Software Licensing > Reports > Usage Data Files。
 4. Click Upload Usage Data。浏览到文件位置（tar格式的RUM报告），选择，然后点击上传数据(Upload Data)。
-



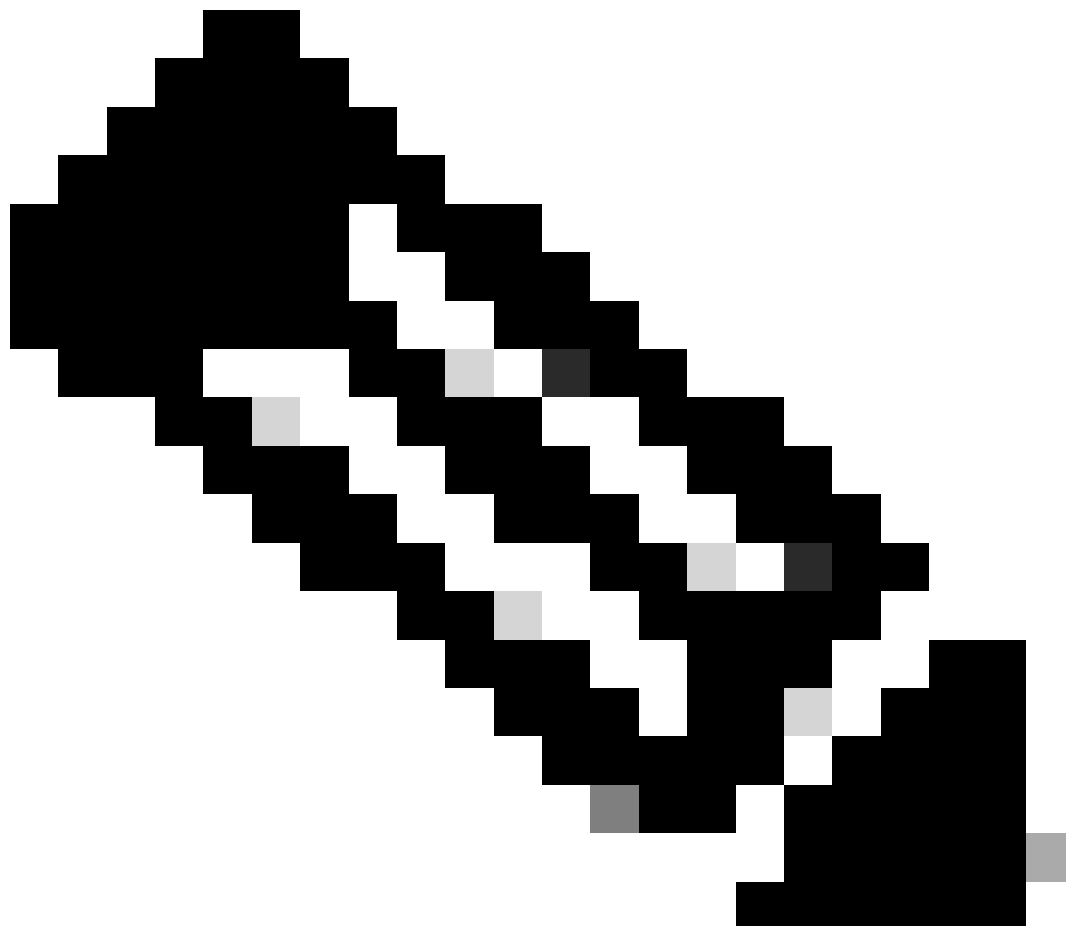
注意：上传文件后，您无法删除该文件。但是，如果需要，您可以上传另一个文件。

5.从Select Virtual Accounts弹出窗口中选择接收已上传文件的虚拟帐户。

6.文件将上传并列于“报告”屏幕的使用数据文件表中。显示的详细信息包括文件名、报告时间、上载

到哪个虚拟帐户、报告状态、报告的产品实例数以及确认状态。

7.在“确认”(Acknowledgement)列中，单击下载以保存您上传的报告或请求的ACK文件。



注意：您必须等待文件出现在“确认”(Acknowledgement)列。如果有许多RUM报告或请求需要处理，Cisco SSM必须花费几分钟。

下载文件后，导入该文件并将其安装在产品实例上

复制信任ACK文件

将文件从其源位置或目录复制到产品实例的闪存中。

CLI 配置：

```
device#copy ftp: flash:
```

```
Address or name of remote host []? 192.168.1.1
Source filename []? ACK_ trust_request.txt
Destination filename [ACK_ trust_request.txt]?
Accessing ftp://192.168.1.1/ACK_ trust_request.txt...!
[OK - 5254/4096 bytes]
```

```
5254 bytes copied in 0.045 secs (116756 bytes/sec)
```

导入该文件并将其安装在产品实例上。

CLI 配置：

```
device#license smart import flash:ACK_ trust_request.txt
Import Data Successful
```

```
device#
```

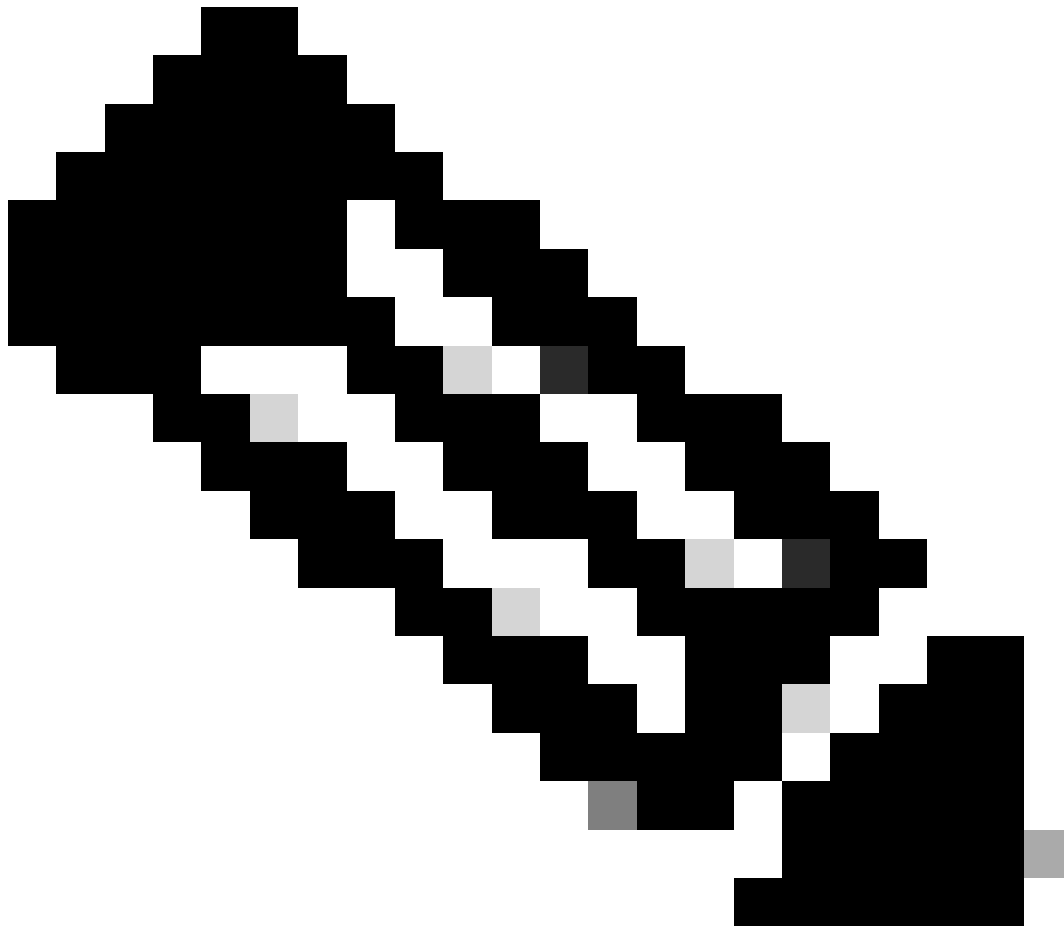
```
*Jun 12 20:01:07.348: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully i
```

安装包包含所有必需信息的授权请求。

在闪存中生成并保存活动产品实例的授权请求。

CLI 配置：

```
device#license smart authorization request add hseck9 all
```



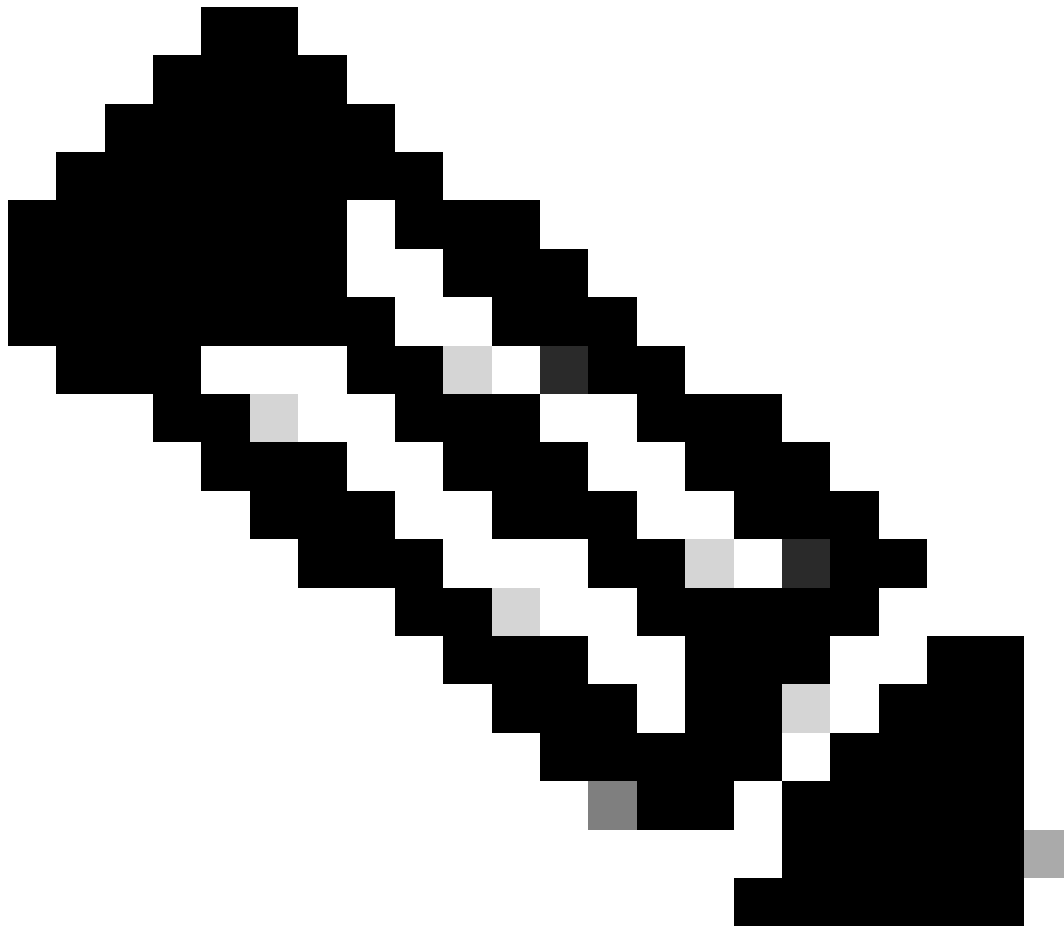
注意：HSEC:高度安全.

将活动产品实例的授权码请求保存在闪存中。

```
device#license smart authorization request save bootflash:auth3.txt
```

将授权请求文件上传到思科SSM并下载ACK文件。

1. 登录Cisco SSM Web UI，网址为<https://software.cisco.com>。在智能软件许可下，单击管理许可证链接。
2. 选择接收报告的智能帐户。
3. 选择Smart Software Licensing > Reports > Usage Data Files。
4. Click Upload Usage Data。浏览到文件位置（tar格式的RUM报告），选择，然后点击上传数据(Upload Data)。

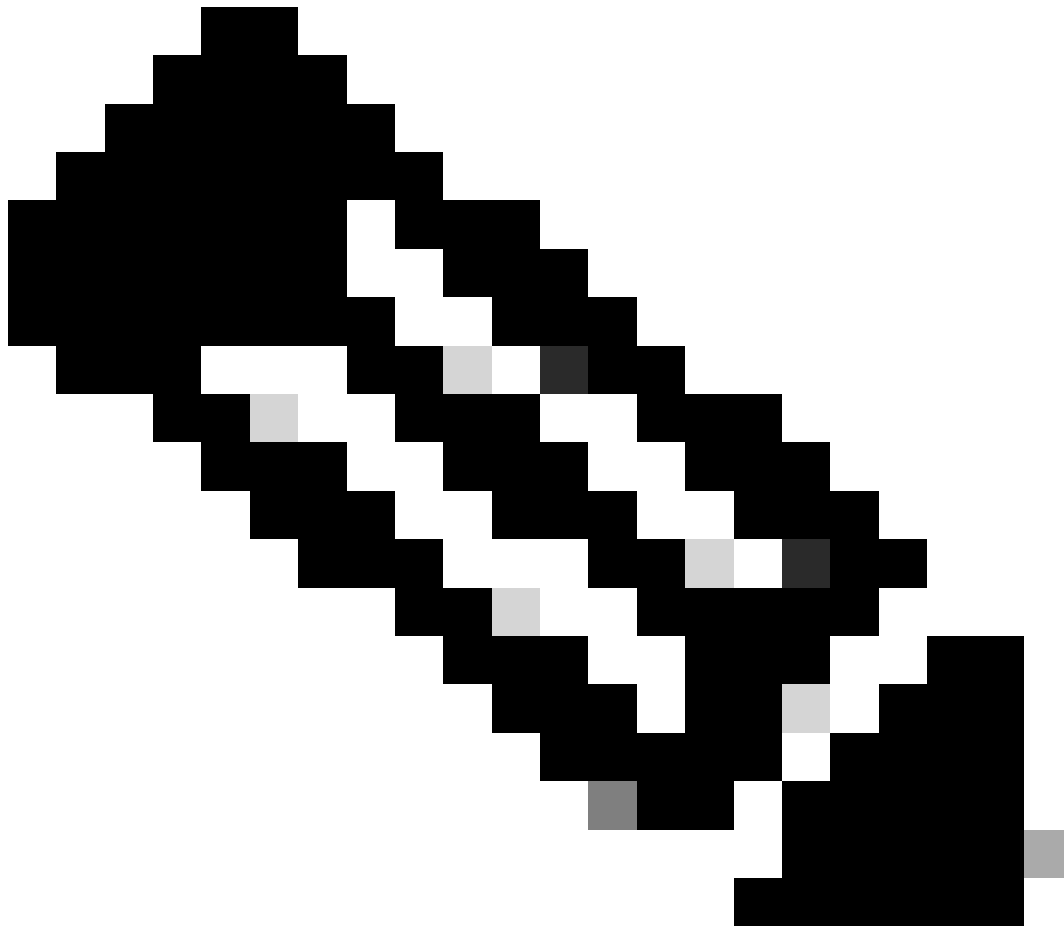


注意：上传文件后，您无法删除该文件。但是，如果需要，您可以上传另一个文件。

5.从Select Virtual Accounts弹出窗口中选择接收已上传文件的虚拟帐户。

文件会上传并列在“报告”(Reports)屏幕的使用数据文件表中。显示的详细信息包括文件名、报告时间、上载到哪个虚拟帐户、报告状态、报告的产品实例数以及确认状态。

6.在“确认”列中，单击下载以保存您上传的报告或请求的ACK文件。



注意：您必须等待文件出现在“确认”(Acknowledgement)列。如果有许多RUM报告或请求需要处理，Cisco SSM必须花费几分钟。

下载文件后，导入该文件并将其安装在产品实例上

CopyAuthorization请求ACK文件

将文件从其源位置或目录复制到产品实例的闪存中。

```
device#copy ftp flash
```

```
Address or name of remote host [192.168.1.1]? 192.168.1.1
```

```
Source filename [ACK_auth3.txt]? ACK_auth3.txt
```

```
Destination filename [ACK_auth3.txt]?
```

```
Accessing ftp://192.168.1.1/ACK_auth3.txt ...!
```


[OK - 1543/4096 bytes]

1543 bytes copied in 0.041 secs (37634 bytes/sec)

InstallAuthorization请求ACK文件

```
device#license smart import flash:ACK_auth3.txt

Last Confirmation code UDI: PID:C9300X-24Y,SN:XXXXXXXXXX

    Confirmation code: a4a85361

Import Data Completed

Last Confirmation code UDI: PID:C9300X-24Y,SN:XXXXXXXXXX

    Confirmation code: a4a85361

device#

*Jun 12 20:05:33.968: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code wa
```

验证

您可以使用以下命令验证许可证状态：

```
device#sh license sum

Account Information:

    Smart Account: Cisco Systems, TAC As of Jun 12 20:03:03 2025 UTC

    Virtual Account: LANSW

License Usage:
```

License	Entitlement Tag	Count	Status

network-advantage	(C9300X-12/24Y Network ...)	1	IN USE
dna-advantage	(C9300X-12/24Y DNA Adva...)	1	IN USE
C9K HSEC	(Cat9K HSEC)	0	NOT IN USE

device#show license authorization

Overall status:

Active: PID:C9300X-24Y,SN:XXXXXXXXXX

Status: SMART AUTHORIZATION INSTALLED on Jun 12 20:05:33 2025 UTC

Last Confirmation code: a4a85361

Authorizations:

C9K HSEC (Cat9K HSEC):

Description: HSEC Key for Export Compliance on Cat9K Series Switches

Total available count: 4

Enforcement type: EXPORT RESTRICTED

Term information:

Active: PID:C9300X-24Y,SN:FJC28281AE2

Authorization type: SMART AUTHORIZATION INSTALLED

License type: PERPETUAL

Term Count: 4

device#sh license all | i Trust

Trust Code Installed: Jun 12 20:01:07 2025 UTC

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。